



THREAT INTELLIGENCE
REPORT

TheProject Casino / OFEDREX / WinSystems

22-domain crypto casino scam network with 383 confirmed victims across 30+ countries

PUBLISHED

March 08, 2026

THREAT TYPE

Casino Scam Network

CLASSIFICATION

TLP:CLEAR

**SEVERITY:
CRITICAL**

PHISHDESTROY RESEARCH DIVISION • [HTTPS://PHISHDESTROY.IO](https://phishdestroy.io) • REPORT ID: PD-THEPROJECT-CASINO-2026-

383

VICTIMS

22

DOMAINS

30+

COUNTRIES

11

PROMO CODES

Executive Summary

TheProject Casino, also known as OFEDREX or WinSystems, is a fake crypto casino and investment scam discovered in January 2026. It is currently active and operates under the brand WinSystems. The scam involves 22 phishing domains and has affected 383 victims across more than 30 countries.

The scam is orchestrated through a panel hosted at `ofedrex.com`, utilizing a Laravel PHP backend. The operation remains active, with ongoing efforts to deceive new victims through fake promotional campaigns and fraudulent winnings.

Threat Actor Profile

TELEGRAM HANDLE	ID	REGISTRATION DATE	ROLE
@project	Unknown	Unknown	Coordinator

Known infrastructure connections include the use of Cloudflare for CDN and protection services.

Technical Infrastructure

COMPONENT	DETAILS
Frontend	Unknown
Backend	Laravel PHP
Authentication	Custom API
CDN	Cloudflare
Hosting	Unknown

API endpoints include:

- `/backend-api/auth/me`
- `/backend-api/worker/users/list`
- `/backend-api/admin/users/list`
- `/backend-api/admin/deposits`
- `/backend-api/admin/settings`

- [/backend-api/admin/logs](#)

Panel sections and configuration parameters include a minimum deposit of \$5 and a required deposit of \$5 for withdrawal verification.

Attack Chain / Scam Flow

1. Victims receive promo codes via social media or Telegram.
2. Victims register on fake casino sites such as [spacema.bet](#) and [lurexcoin.com](#).
3. Fake "winnings" are displayed to build trust with the victims.
4. Victims are required to deposit cryptocurrency for "withdrawal verification."
5. Funds are stolen, and the withdrawal is never processed.

Indicators of Compromise

DOMAIN	STATUS
spacema.bet	Active
lurexcoin.com	Active
ofedrex.com	Panel
money-king.bet	Active
mogulbet.vip	Active
xwebet.com	Active
axidex.com	Active
sho.mom	Active
bitfirefox.com	Active
infocryptox.com	Active
merbibet.com	Active
greencasino.bet	Active
goldix.bet	Active
bolterex.com	Active
evbobet.top	Active
explay.bet	Active
fortexo.top	Active
inclusivebets.fun	Active
luckberry.run	Active
testpet.icu	Test
www.casinopro.fit	Active
www.spacema.bet	Alias

Victim Impact

COUNTRY	VICTIMS	PERCENTAGE
India	77	20.1%
Hungary	45	11.7%
Poland	40	10.4%
Romania	25	6.5%
United States	24	6.3%
Netherlands	24	6.3%
Germany	21	5.5%
Indonesia	12	3.1%
Finland	11	2.9%
France	9	2.3%

Promo code analysis shows that the code **DREAM** was used by 115 victims, primarily sourced from social media campaigns.

MITRE ATT&CK Mapping

TACTIC	TECHNIQUE ID	TECHNIQUE NAME	EVIDENCE
Initial Access	T1566	Phishing	Promo codes distributed via social media
Credential Access	T1078	Valid Accounts	Credentials for worker accounts leaked
Exfiltration	T1041	Exfiltration Over C2 Channel	Funds transferred to scammer-controlled wallets

Countermeasures

- End users should verify the legitimacy of online casinos before registering.
- SOC teams should monitor for promo codes like **DREAM** and **LRX774** in network traffic.
- Registrars should be notified to take down fraudulent domains.
- Law enforcement should be informed about the scam's infrastructure and victim impact.
- Use the [PhishDestroy free domain scanner](#) to identify risky domains.
- Refer to the [DestroyList open-source blocklist](#) for updated threat data.

References

- [PhishDestroy threat intelligence platform](#)
- [Free domain risk scanner](#)
- [DestroyList community-maintained blocklist](#)
- [ScamIntelLogs evidence archive](#)

Download IOCs (CSV)

